# 編 者 的 話

数学课外读物对于帮助学生学好数学，扩大他们的数学知识领域，是很有好处的．近年来，越来越多的中学学生和教师，都迫切希望出版更多的适合中学生阅读的通俗数学读物．我们约请一些数学工作者，编了这套“数学小丛书”，陆续分册出版，来适应这个要求．

这套书打算介绍一些课外的数学知识，以扩大学生的知识领域，加深对数学基础知识的掌握，引导学生独立思考，理论联系实际。

这是我们的初步想法和尝试．热切地希望数学工作者和读者对我们的工作提出宝贵的意见和建议，更希望数学工作者为中学生写出更多更好的数学课外读物。

北京市数学会

1962 年 4 月

扌

甲

三人同行七十稀，

五树梅花廿一枝，

七子团圆月正半，

除百零五便得知.

——程大位，算法統宗(1583).

# 序

神奇妙算古名詞，
　师承前人沿用之，
神奇化易是坦道，
　易化神奇不足提．
妙算还从拙中来，
　愚公智叟两分开，
积久方显愚公智，
　发白才知智叟呆．
埋头苦干是第一，
　熟练生出百巧来，
勤能补拙是良訓，
　一分辛劳一分才．

华 罗 庚　1963年2月11日于北京铁獅子坟．

# 目　次


一　問題的提出……1

二　"笨"算法……2

三　口訣及其意义……5

四　輾轉相除法……7

五　一些說明……10

六　插入法……12

七　多項式的輾轉相除法……14

八　例子……16

九　实同貌异……17

十　同余式……19

十一　一次不定方程……22

十二　原則……25

附記　孙子算經……27

# 一　問題的提出

“孙子算經”是我国古代的一部优秀数学著作，确切的出版年月无从考证．其中有“物不知其数”一問，原文如下：

“今有物不知其数，三三数之賸二，五五数之賸三，七七数之賸二，問物几何？”

这个問題的意义可以用以下的数学游戏来表达：

有一把圍棋子，三个三个地数，最后余下两个，五个五个地数，最后余下三个，七个七个地数，最后余下二个．問这把棋子有多少个？

这类的問題在我国古代数学史上有不少有趣味的名称．除上面所說的“物不知其数”而外，还有称之为“鬼谷算”的，“秦王暗点兵”的．还有“剪管术”，“隔墙算”，“神奇妙算”，“大衍求一术”，等等．

这个問題的算法是用前面程大位的四句詩来概括的．这个問題和它的解法是世界数学史上著名的东西，一般称它为孙子定理，或中国余数定理．这一工作不仅在古代数学史上占有地位，而且这个問題的解法的原則在近代数学史上还占有重要的地位，在电子計算机的設計中也有重要的应用．

这个問題属于数学的一个分支——数論．但方法的原則却反映在插入理論、代数理論及算子理論（泛函分析）之中．

学好初等数学，融会貫通，会对将来学好高等数学提供簡单而具体的模型的.

这个問題难不难？不难！高小初中的学生都可以学会. 但由此所启发出来的东西却是这本小册子所不能介紹的了.

我准备先讲一个笨办法——“笨”字可能用得不妥当，但这个方法是朴素原始的方法，算起来費时間的方法. 其次讲解我国古代原有的巧方法. 然后讲这巧方法所引伸出来的一些中学生所看得懂的东西——面目全非，原則則一. 这样发現同一性，正是数学訓练的重要部分之一. 最后談談这个問題所启发出来的一支学問——同余式理論的簡单介紹.

## 二 “笨”算法

原来的問題是：求一数，三除余二，五除余三，七除余二. 这問題太容易回答了，因为三除余二，七除余二，則二十一除余 2，而 23 是三、七除余二的最小数，剛好又是五除余三的数. 所以心算快的人都能算出. 我們还是换一个例子吧！

我們来試图解决：三除余二，五除余三，七除余四的問題. 我們先介紹以下的笨算法.

在算盘上先打上(或紙上写上)2，每次加三，加成五除余三的时候暫停下来，再在这个数上每次加 15，到得出 7 除余 4 的数的时候，就是答数. 具体地說：从 2 加 3，再加 3 得 8，即

$$2,\ 2+3=5,\ 5+3=8,$$

它是 5 除余 3 的数. 然后在 8 上加 15，再加 15，第三次加 15，

得 53, 即

$$8,\ 8+15=23,\ 23+15=38,\ 38+15=53.$$

它是第一个 7 除余 4 的数. 53 就是解答. 經过驗算, 正是 53, 3 除余 2, 5 除余 3, 7 除余 4.

这方法的道理是什么? 很簡单: 先从 3 除余 2 的数中去找 5 除余 3 的数. 再从"3 除余 2, 5 除余 3"的数中去找 7 除余 4 的数, 如此而已. 这方法虽然拙笨些, 但这是一个步步能行的方法, 是一个值得推荐的、朴素的方法.

但注意, 問題的提法是有問題的. 不但 53 有此性质, 53+105=158, 158+105=263 都有此性质. 确切的提法应当是: 求出三除余二, 五除余三, 七除余四的最小的正整数.

讀者試一下: 三除适尽, 五除余二, 七除余四的問題. 讀者将发現計算較麻煩了! 在练几次之后便会发現, 在計算的过程中从"大"除数出发可能算得快些: 先看 7,

$$4,\ 4+7=11,\ 11+7=18,\ 18+7=25,\ 25+7=32.$$

这是第一个五除余二的数. 再由

$$32,\ 32+35=67,\ 67+35=102$$

即得所求.

总之: 第一法"3, 5, 7"法, 是从問題本身立刻反映出来的方法. 再思考一下, 每次加得大, 則算得快, 因此得第二法"7, 5, 3"法. 由于 5 的余数一目了然, 因而用"7, 3, 5"法也可能省劲些. 总之, 先不要以为方法笨, 有了方法之后, 方法是死的, 人是活的. 运用之妙, 存乎其人.

我們再介紹一个麻煩得多的問題. 这也是古代的現成問

題，見黃宗宪著的“求一术通解”。原文如次:

“今有数不知总；以五累减之无賸，以七百十五累减之賸十，以二百四十七累减之賸一百四十，以三百九十一累减之賸二百四十五，以一百八十七累减之賸一百零九。問总数若干”。

好麻煩的問題．但看两遍問題之后立刻发現，有窍門在！第一句“以五累减之无賸”是廢話，因为哪一个715除余10的数不是五的倍数．第三句話，因为余数140是5的倍数，而原数又是五的倍数，因此这句話可以改为“$247\times5=1235$累减之賸140．同法第四句也可以改为“$391\times5=1955$累减之賸245.

我們現在从1955除余245，1235除余140出发.

245，$245+1955=2200$，4155，6110，8065，10020，

245，　　　　　　965，　450，1170，　655，　140.

下一行是上一行的数除1235所得的余数，依次試除，发現10020就是黃宗宪所要求的答案了

看来煩得可怕，算来不过尔尔．多动动手，多动动脑子，便会熟能生巧.

在楊輝著的《續古摘奇算法(1275)》上还有以下的例子：

“二数余一，五数余二，七数余三，九数余四，問本数.”

首句与末句合起来是“18除余13”，再由

$$13,\ 13+18=31,\ 31+18=49,\ 49+18=67,$$

67是五除余2的数，再由

$$67,\ 67+5\times18=67+90=157,$$

157就是解答了。

在楊輝的书上还有以下二問:

七数剩一，八数剩二，九数剩三，問本数.

十一数余三，十二数余二，十三数余一，問本数.

讀者請暫勿动手，細看一下！看看能不能不用复杂計算(或就用心算)給出这两个問題的解答来.

更考慮以下的問題：有 $n$ 个正整数 $a_1, \cdots, a_n$. 求最小的正整数之被 $a_1$ 除余 $a_1-p$，被 $a_2$ 除余 $a_2-p, \cdots$，被 $a_n$ 除余 $a_n-p$ 者.

求最小的正整数，被 $a_1$ 除余 $l-a_1$，被 $a_2$ 除余 $l-a_2, \cdots$，被 $a_n$ 除余 $l-a_n$ 者.

这两个題形式上吓唬人，但实质上与楊輝原来的問題并无太大的差异.

## 三　口訣及其意义

“三人同行七十稀，五树梅花廿一枝，

七子团圓月正半，除百零五便得知.”

这几句口訣見程大位著的《算法統宗》. 它的意义是:

用 70 乘 3 除所得的余数，21 乘 5 除所得的余数，15 乘 7 除所得的余数，然后总加起来. 如果它大于 105，則减 105，还大再减，…最后得出来的正整数就是答数了.

以孙子算經上的例子来說明. 它的形式是

$$2\times70+3\times21+2\times15=233.$$

两次减去 105，得 23. 这就是答数了！

(讀者試算一下第二节开始的另一个例子.)

为什么 70, 21, 15 有此妙用? 这 70, 21, 15 是怎样求出来的?

先看 70,21,15 的性质: 70 是这样一个数, 3 除余 1, 5 与 7 都除得尽的数. 所以 $70a$ 是一个 3 除余 $a$ 而 5 与 7 除都除得尽的数. 21 是 5 除余 1, 3 与 7 除尽的数, 所以 $21b$ 是 5 除余 $b$ 而 3 与 7 除得尽的数. 同样, $15c$ 是 7 除余 $c$ 而 3 与 5 除得尽的数. 总起来

$$70a+21b+15c$$

是一个 3 除余 $a$, 5 除余 $b$, 7 除余 $c$ 的数, 也就是可能的解答之一, 但可能不是最小的. 这数加减 105 都仍然有同样性质. 所以可以多次减去 105 而得出解答来.

在程大位的口訣里, 前三句的意义是点出 3、5、7 与 70、15、21的关系, 后一句說明为了寻求最小正整数解还須减105, 或再减 105 等.

(讀者自证, 这一方法頂多只須要减两个 105, 而不会要减三个 105.)

这个方法好是好, 但人家是怎样找出这 70、21、15 来的. 当然可以凑, 在算盘上先打上 35, 它不是 3 除余 1. 再加上 35 得 70, 它是 3 除余 1 了. 其它仿此.

但这是 3、5、7, 凑来容易! 一般如何? 例如 4、6、9, 我們不难发現, 并沒有 4 除余 1, 6 除、9 除余 0 的数存在. 欲知求出 70、21、15 的一般方法, 且看下文.

# 四　輾轉相除法

我們所要求的数是：3 除余 1，35(=5×7)除余 0 的数．也就是要找 $x$，使 $35x$ 是 3 除余 1 的数，也就是它等于 $3y+1$．直截地說，就是要找 $x$、$y$，使

$$35x-3y=1.$$

这个方程怎样解？閱讀过我写的《从祖冲之的圓周率談起》* 一书的讀者，一定知道解法：把$\frac{35}{3}$展开为連分数 $11+\frac{2}{3}=11+\frac{1}{1}+\frac{1}{2}$，而漸近連分数是 $11+\frac{1}{1}=\frac{12}{1}=\frac{u}{v}$，由此得出

$$35v-3u=-1$$

来．因此 $35(3-v)-3(35-u)=1$，因而 $x=3-v=2$，$y=35-u=23$ 就是解答(即 $35\times2-3\times23=1$)．因而 $35x=70$ 就是所求的数了．

也許有些讀者沒有看过我那本小册子．好在問題不比那本书上更复杂，我們还是从輾轉相除法談起．輾轉相除法是用来求最大公約数的．我們用代数的形式来表达(实质上，算术形式也是可以完全讲得清楚的)．

給出两个正整数 $a$ 和 $b$，用 $b$ 除 $a$ 得商 $a_0$，余数 $r$，写成式子

$$a=a_0b+r,\quad 0\leqslant r<b. \tag{1}$$

这是最基本的式子，輾轉相除法的灵魂．如果 $r$ 等于 0，那么 $b$ 可以除尽 $a$，而 $a$、$b$ 的最大公約数就是 $b$．

---

* 《从祖冲之的圓周率談起》是这套小丛书之(3)。

如果 $r\neq 0$, 再用 $r$ 除 $b$, 得商 $a_1$, 余数 $r_1$, 即

$$b=a_1r+r_1,\quad 0\leqslant r_1<r. \tag{2}$$

如果 $r_1=0$, 那么 $r$ 除尽 $b$, 由(1)也除尽 $a$, 所以 $r$ 是 $a$、$b$ 的公約数. 反之, 任何一个除尽 $a$、$b$ 的数, 由(1), 也除尽 $r$, 因此 $r$ 是 $a$、$b$ 的最大公約数.

如果 $r_1\neq 0$, 則用 $r_1$ 除 $r$ 得商 $a_2$, 余数 $r_2$, 即

$$r=a_2r_1+r_2,\quad 0\leqslant r_2<r_1. \tag{3}$$

如果 $r_2=0$, 那么由(2)可知 $r_1$ 是 $b$、$r$ 的公約数, 由(1), $r_1$ 也是 $a$、$b$ 的公約数. 反之, 如果一数除得尽 $a$、$b$, 那末由(1), 它一定也除得尽 $b$、$r$, 由(2), 它一定除得尽 $r$、$r_1$, 所以 $r_1$ 是 $a$、$b$ 的最大公約数.

如果 $r_2\neq 0$, 再用 $r_2$ 除 $r_1$, 如法进行. 由于 $b>r>r_1>r_2>\cdots$ 逐步小下来, 而又都是正整数, 因此經过有限步驟后一定可以找到 $a$、$b$ 的最大公約数 $d$ (它可能是 1). 这就是有名的**輾轉相除法**, 在外国称为欧几里得算法. 这个方法不但給出了求最大公約数的方法, 而且帮助我們找出 $x$、$y$, 使

$$ax+by=d. \tag{4}$$

在說明一般道理之前, 先看下面的例子.

从求 42897 与 18644 的最大公約数出发:

$$42897=2\times 18644+5609, \tag{i}$$

$$18644=3\times 5609+1817, \tag{ii}$$

$$5609=3\times 1817+158, \tag{iii}$$

$$1817=11\times 158+79, \tag{iv}$$

$$158=2\times 79.$$

这样求出最大公約数是 79. 我們現在来寻求 $x$、$y$, 使 $42897x+18644y=79$. 由(iv)可知

$$1817-11\times158=79.$$

把(iii)式的 158 表达式代入此式, 得

$$79=1817-11(5609-3\times1817)$$
$$=34\times1817-11\times5609.$$

再以(ii)式的 1817 表达式代入, 得

$$79=34\times(18644-3\times5609)-11\times5609$$
$$=34\times18644-113\times5609.$$

再以(i)式的 5609 表达式代入, 得

$$79=34\times18644-113\times(42897-2\times18644)$$
$$=260\times18644-113\times42897.$$

也就是 $x=-113$, $y=260$.

这虽然是特例, 也說明了一般的理論. 一般的理論是: 把輾轉相除法写成为

$$a=a_0b+r,$$
$$b=a_1r+r_1,$$
$$r=a_2r_1+r_2,$$
$$r_1=a_3r_2+r_3,$$
$$\cdots\cdots\cdots\cdots$$
$$r_{n-1}=a_{n+1}r_n+r_{n+1},$$
$$r_n=a_{n+2}r_{n+1}.$$

这样得出最大公約数 $d=r_{n+1}$. 由倒数第二式, $r_{n+1}$ 可以表为 $r_{n-1}$、$r_n$ 的一次式, 再倒回一个可以表为 $r_{n-2}$、$r_{n-1}$ 的一次

式，…，最后表为 $a$、$b$ 的一次式.

我們試用这个方法把“3、5、7”算改为“3、7、11”算.

先求 3 除余 1，77 除尽的数. 3 除 77 余 2，因此 154 就是. 不必算.

再求 7 除余 1，33 除尽的数. 用輾轉相除法

$$33-4\times7=5,\ 7-5=2,\ 5-2\times2=1.$$

因此

$$\begin{aligned}1&=5-2\times2=5-2(7-5)=3\times5-2\times7\\&=3(33-4\times7)-2\times7=3\times33-14\times7.\end{aligned}$$

即对应的数是 99.

最后求 11 除余 1，21 除尽的数. 11 除 21 得商 2 余 $-1$. 因此 $11\times21-21=210$ 就是所求的数. 因此得出“3、7、11”算的結論如下:

三对么五四，七对九十九，

十一、二百十，減数二三么.

## 五　一些說明

我們再发揮一下楊輝的例子.

“二除余 $a$，五除余 $b$，七除余 $c$，九除余 $d$，求本数.”

二对应的系数是 $5\times7\times9=315$，

五对应的系数是 $2\times7\times9=126$，

七对应的系数求法如下：$2\times5\times9=90$，七除余 $-1$，因此 $90\times6=540$ 就是 2，5，9 除尽，7 除余一的数了.

九对应的系数求法如下：对 70 与 9 用輾轉相除法（变着!）. $70-9\times8=-2$， $9-4\times2=1$，因此

$$1=9-4\times2=9+4\times(70-9\times8)=4\times70-31\times9,$$

即 $4\times70=280$ 是对应的系数。

因此問題的解答是：

$$315a+126b+540c+280d$$

减去 $2\times5\times7\times9=630$ 的倍数.

再举一个例子.

"四除余 $a$，六除余 $b$，九除余 $c$，求本数."

上法不能进行，因为沒有 6，9 除尽而 4 除余一的数！同时这类的問題也眞可能沒有解，例如：$a$ 是偶数，$b$ 是奇数．又如，$b$ 是三的倍数，而 $c$ 不是！这样的問題如何解？当然开始介紹的"笨"办法还是可行．但无解时却就苦了！这样問題必先注意这些除数的公因子問題．首先，$a$、$b$ 必須同时为奇或为偶，其二，$b$、$c$ 必須对三有相同的余数．否則无解．

如果这些条件适合了，我們就可以考虑求解問題．对本問題来說，由第一个条件决定了 $b$ 的奇偶性，由第三个条件决定了 $b$ 被 3 除所得的余数，因而确定了 $b$ 被 6 除的余数．因而第二个条件是多余的．也就是：除非原問題无解答．要有一定是

"四除余 $a$，九除余 $c$"的数了．（答数是 $9a-8c$ 加减 36 的倍数）

因此，解問題的时候：先看諸除数，有无公因子，对于公因子，必須要同余.

为了考虑得更細致些，我們引入以下的反問題：如果一数被 $ab$ 除之余 $c$，則可由之知道它被 $a$ 除余几，$b$ 除余几．例如：6 除余 4 的数一定是 2 除适尽，3 除余 1．反之，2 除适尽，3 除余 1 的数也是 6 除余 4 的数．这样便可拆开来再合并起来看了．

例如：求 6 除余 4，10 除余 8，9 除余 4 的数．

拆开来，第一句話是"2 除适尽，3 除余 1"，第二句話是"2 除适尽，5 除余 3"，第三句話是"3 除余 1，9 除余 4"．（拆法有些不同，必須注意）綜合起来就是：

"2 除适尽，5 除余 3，9 除余 4．"（答数 58）如果經分析后有矛盾出現，就无解．

## 六 插入法

以上所介紹的神奇妙算中的（70、21、15）法，給我們提供出一个数学上很有用的原則和方法．在抽象地刻划这个原則和方法之前，还是先讲些应用，甚至于讀者看穿了这点之后，可以不必再讲原則，而自己也会体会到的．

問題：要找出一个函数在 $a$、$b$、$c$ 三点取数值 $\alpha$、$\beta$、$\gamma$．

孙子方法給我們提供解决这問題的途徑：先作一个函数 $p(x)$ 在 $a$ 点等于 1，在 $b$、$c$ 点都等于 0；再作 $q(x)$ 在 $b$ 点等于 1，在 $c$、$a$ 点都等于 0；然后作 $r(x)$ 在 $c$ 点等于 1，而在 $a$、$b$ 点都等于 0．这样

$$\alpha p(x)+\beta q(x)+\gamma r(x)$$

就适合要求了!

最簡单的 $p(x)$ 定法如下: 它既然在 $b$、$c$ 处为 0, 则

$$p(x)=\lambda(x-b)(x-c).$$

又由 $p(a)=1$, 可得

$$p(x)=\frac{(x-b)(x-c)}{(a-b)(a-c)}.$$

同法得出

$$q(x)=\frac{(x-c)(x-a)}{(b-c)(b-a)},\quad r(x)=\frac{(x-a)(x-b)}{(c-a)(c-b)}.$$

因此

$$\alpha\frac{(x-b)(x-c)}{(a-b)(a-c)}+\beta\frac{(x-c)(x-a)}{(b-c)(b-a)}+\gamma\frac{(x-a)(x-b)}{(c-a)(c-b)} \quad (A)$$

就是問題的一个解答.

(A)是著名的插入法中的 Lagrange 公式. 从孙子的原則来看, 推导是多么簡单明了.

数学在应用的时候, 一般仅仅有有限个数据, 我們就用这一类的方法来推演出函数来. 来描述其他各点的大概数据.

一般的插入法公式是:

在 $n$ 个不同点 $a_1, \cdots, a_n$, 函数 $f(x)$ 各取值 $\alpha_1, \cdots, \alpha_n$ 的插入公式是

$$\alpha_1\frac{(x-a_2)\cdots(x-a_n)}{(a_1-a_2)\cdots(a_1-a_n)}$$
$$+\alpha_2\frac{(x-a_1)(x-a_3)\cdots(x-a_n)}{(a_2-a_1)(a_2-a_3)\cdots(a_2-a_n)}+\cdots$$
$$+\alpha_n\frac{(x-a_1)\cdots(x-a_{n-1})}{(a_n-a_1)\cdots(a_n-a_{n-1})}.$$

这是不必证明的公式了！

由此看来“插入公式”与“70, 21, 15”法，面貌虽不同，原则本无隔.

那儿可以差一个105的倍数，而这儿可以差一个在 $a_1, \cdots, a_n$ 点都等于0的函数.

## 七　多項式的輾轉相除法

整数固然有輾轉相除法的現象，多項式也有相似的性质. 假定 $a(x)$ 与 $b(x)$ 是两个多项式. 用 $b(x)$ 除 $a(x)$ 得商式 $a_0(x)$，得余式 $r(x)$，也就是

$$a(x)=a_0(x)b(x)+r(x),$$

而 $r(x)$ 的次数小于 $b(x)$ 的次数. 如果 $r(x)\equiv 0$，則 $a(x)$、$b(x)$ 的最大公因式就是 $b(x)$.

如果 $r(x)\not\equiv 0$，則以 $r(x)$ 除 $b(x)$ 得商式 $a_1(x)$，余式 $r_1(x)$，即

$$b(x)=a_1(x)r(x)+r_1(x),$$

而 $r_1(x)$ 的次数小于 $r(x)$ 的次数. 如果 $r_1(x)\equiv 0$，則 $r(x)$ 就是 $a(x)$ 与 $b(x)$ 的最大公因式.

如果 $r_1(x)\not\equiv 0$，則以 $r_1(x)$ 除 $r(x)$ 得

$$r(x)=a_2(x)r_1(x)+r_2(x),$$

$r_2(x)$ 的次数小于 $r_1(x)$ 的次数. 这样一直下去，得出一系列的多项式

$$r(x),\ r_1(x),\ r_2(x),\cdots$$

它們的次数一个比一个小，当然不能无限下去，一定有时候会出現

$$r_{n-1}(x)=a_{n+1}(x)r_n(x)+r_{n+1}(x)$$

及

$$r_n(x)=a_{n+2}(x)r_{n+1}(x)$$

的現象。这样便可以得出：$r_{n+1}(x)$是$a(x)$与$b(x)$的最大公因式（证明让讀者自己补出）。同样不难证明，如果$d(x)$是$a(x)$，$b(x)$的最大公因式，則一定有两个多項式$p(x)$与$q(x)$，使

$$a(x)p(x)+b(x)q(x)=d(x).$$

特别有：如果$a(x)$和$b(x)$无公因式，則有$p(x)$与$q(x)$使

$$a(x)p(x)+b(x)q(x)=1.$$

多項式既然有这一性质，就启发出应当有多項式的"神奇妙算"。

例如：有三个无公因子的多項式$p(x)$、$q(x)$、$r(x)$，求出一个多項式$f(x)$使$p(x)$、$q(x)$、$r(x)$除之各余$a(x)$、$b(x)$、$c(x)$。并且要$f(x)$的次数最低。

根据孙子原則：先找出$q(x)$、$r(x)$除尽而$p(x)$除余1的多項式$A(x)$；再找出$r(x)$、$p(x)$除尽而$q(x)$除余1的多項式$B(x)$；更找出$p(x)$、$q(x)$除尽而$r(x)$除余1的多項式$C(x)$。則

$$A(x)a(x)+B(x)b(x)+C(x)c(x)$$

就是$p(x)$、$q(x)$、$r(x)$除各余$a(x)$、$b(x)$、$c(x)$的多項式。但并非最低次。再以$p(x)q(x)r(x)$除之，所得出的余式就是最低

次的适合要求的多項式了.

## 八 例子

例: 求出 $x+1$ 除余 1, $x^2+1$ 除余 $x$, $x^4+1$ 除余 $x^3$ 的次数最低的多項式.

先找出 $x^2+1$、$x^4+1$ 除得尽而 $x+1$ 除余 1 的多項式. 一找就到: $\frac{1}{4}(x^2+1)(x^4+1)$. 这就是我們所求的 $A(x)$.

再找出 $x+1$、$x^4+1$ 除得尽, 而 $x^2+1$ 除余 1 的多項式. 用輾轉相除法, 得

$$(x+1)(x^4+1)-(x^3+x^2-x-1)(x^2+1)=2x+2.$$

$$x^2+1-\left[\frac{1}{2}(x-1)\right](2x+2)=2.$$

因此

$$\begin{aligned}2&=(x^2+1)-\left[\frac{1}{2}(x-1)\right](2x+2)\\&=(x^2+1)-\left[\frac{1}{2}(x-1)\right]\Big[(x+1)(x^4+1)-(x^3+x^2-x-\\&\qquad\qquad -1)\times(x^2+1)\Big]\\&=\left[\frac{1}{2}(x-1)(x^3+x^2-x-1)+1\right](x^2+1)-\frac{1}{2}(x-1)\times\\&\qquad\qquad\times(x+1)(x^4+1).\end{aligned}$$

以 2 除之, 得出 $B(x)=-\frac{1}{4}(x-1)(x+1)(x^4+1)$.

再找出 $x+1$、$x^2+1$ 除得尽, 而 $x^4+1$ 除余 1 的多項式.

立刻看出

$$(x-1)[(x+1)(x^2+1)]-(x^4+1)=-2.$$

即 $$C(x)=-\frac{1}{2}(x-1)(x+1)(x^2+1).$$

因此 $$a(x)A(x)+b(x)B(x)+c(x)C(x)$$

$$=\frac{1}{4}(x^2+1)(x^4+1)-\frac{1}{4}(x-1)(x+1)(x^4+1)x$$

$$-\frac{1}{2}(x^2-1)(x^2+1)x^3$$

$$=\frac{1}{4}(-3x^7+x^6+x^5+x^4+x^3+x^2+x+1)$$

加上$\frac{3}{4}(x+1)(x^2+1)(x^4+1)=\frac{3}{4}\cdot\frac{x^8-1}{x-1}=\frac{3}{4}(x^7+x^6+x^5+x^4+x^3+x^2+x+1)$，得出答数

$$x^6+x^5+x^4+x^3+x^2+x+1.$$

大家别以为关于多项式的"神奇妙算"与插入法有何不同．学了插入公式，多学了些东西，实质上并无什么新鲜处．如果不信，請以 $p(x)=x-a$，$q(x)=x-b$，$r(x)=x-c$ 为例．立刻发現 Lagrange 插入公式就是我們这儿所介紹的东西的最簡单的例子．

## 九　实同貌异

### 1）复整数

一个虛实部分都是整数的复数称为复整数．对复整数来說，輾轉相除法还能成立．即任給两个复整数 $\alpha=a_1+a_2i$ 及

$\beta=b_1+b_2i$, 我們可以找出两个复整数

$$\gamma=c_1+c_2i \text{ 与 } \delta=d_1+d_2i$$

使
$$\alpha=\gamma\beta+\delta,\quad |\delta|<|\beta|.$$

根据这一性质, 讀者試試看, 能不能作出相应的結論来.

**2) 多变数内插法**

多变数的插入公式, 我們作如下的建議.

在平面上給了 $n$ 点

$$(x_1, y_1),\ (x_2, y_2), \cdots, (x_n, y_n)$$

求一函数 $f(x, y)$ 在这 $n$ 点各有数值 $\alpha_1, \cdots, \alpha_n$.

根据孙子原理, 我們作出

$$P_1(x, y)=\frac{[(x-x_2)^2+(y-y_2)^2][(x-x_3)^2+(y-y_3)^2]\cdots[(x-x_n)^2+(y-y_n)^2]}{[(x_1-x_2)^2+(y_1-y_2)^2][(x_1-x_3)^2+(y_1-y_3)^2]\cdots[(x_1-x_n)^2+(y_1-y_n)^2]}.$$

这是一个函数在 $(x_2, y_2), \cdots, (x_n, y_n)$ 諸点为 0, 在 $(x_1, y_1)$ 这一点为 1 (当然, 做法不是唯一的, 你可以根据应用上的需要作出这类的函数来. 量子力学里的"$\delta$ 函数"就是根据这样的想法来的). 同样做出

$$P_2(x, y), \cdots, P_n(x, y).$$

而

$$\alpha_1P_1(x, y)+\cdots+\alpha_nP_2(x, y)$$

就是一个在所給点吻合于客观数据的函数.

在数学的应用中, 經常只有有限个数据, 怎样从有限个数据来描述客观的函数. 或者說怎样去找出函数来与客观数据吻合, 又能有大勢地代表客观情况. 这一門学問就是插入法. 必須注意, 插入法所得出的函数毕竟并不一定是眞正的

函数，而是某种近似而已．但也可能提供出可能性，因而理論上加以证明，这就是眞正反映客观情况的函数的时候也还是有的．

## 十　同余式

讲到这儿实际上已經讲了不少同余式的性质了．我們現在可以較系統地介紹同余式理論了．

**定义**　命 $m$ 为一自然数．如果 $a-b$ 是 $m$ 的倍数，則謂之 $a$、$b$ 对模 $m$ 同余．用符号

$$a \equiv b \pmod{m}$$

表之．也就是說，用 $m$ 除 $a$ 及 $b$ 有相同的余数．

例如：$21 \equiv -11 \pmod{8}$．

用同余式符号，孙子問題可以写成为：求 $x$，使

$$x \equiv 2 \pmod{3},$$

$$x \equiv 3 \pmod{5},$$

$$x \equiv 2 \pmod{7}.$$

同余式有以下的一些性质：

(i)　$a \equiv a \pmod{m}$（反身性）；

(ii) 如果 $a \equiv b \pmod{m}$，則 $b \equiv a \pmod{m}$（对称性）；

(iii) 如果 $a \equiv b \pmod{m}$，$b \equiv c \pmod{m}$，則 $a \equiv c \pmod{m}$（傳递性）．

并且还有

(iv) 如果 $a \equiv b \pmod{m}$，$a_1 \equiv b_1 \pmod{m}$，則 $a+a_1 \equiv b+b_1$

$(mod\, m)$及 $a-a_1\equiv b-b_1(mod\, m)$(等式求和差性)。

(v)如果 $a\equiv b$, $a_1\equiv b_1(mod\, m)$則

$$aa_1\equiv bb_1 \ (mod\, m)\text{(等式求积性)}.$$

但需注意,“等式两边不能同除一数”。例如$6\equiv 8(mod\, 2)$,但 $3\not\equiv 4(mod\, 2)$.

**定理** 命$m$是$m_1$、$m_2$的最小公倍数. 同余式

$$x\equiv a_1(mod\, m_1), \tag{1}$$

$$x\equiv a_2(mod\, m_2) \tag{2}$$

有公解的必要且充分条件是$m_1$、$m_2$的最大公約数除得尽$a_1-a_2$. 如果这条件适合,則方程組有一个而且仅有一个小于$m$的非負整数解.

**证明** 1)命$d$是$m_1$、$m_2$的最大公約数. 由(1)、(2)立刻得出

$$x\equiv a_1 \ (mod\, d), \quad x\equiv a_2(mod\, d).$$

等式相减得出$0=a_1-a_2(mod\, d)$. 因此如果(1)、(2)有公解,則$d$一定除尽$a_1-a_2$.

2)反之,如果$d$除尽$a_1-a_2$. 由(1)

$$x=a_1+m_1y, \tag{3}$$

代入(2),得

$$a_1+m_1y\equiv a_2 \ (mod\, m_2).$$

也就是

$$a_1-a_2=m_2z-m_1y.$$

即

$$\frac{a_1-a_2}{d}=\frac{m_2}{d}z-\frac{m_1}{d}y. \tag{4}$$

由于$\frac{m_1}{d}$与$\frac{m_2}{d}$沒有公因子，因此由輾轉相除所推出的結論，一定有 $p, q$ 使

$$1=\frac{m_2}{d}p-\frac{m_1}{d}q. \tag{5}$$

如果取 $z=\frac{a_1-a_2}{d}p$, $y=\frac{a_1-a_2}{d}q$，則(4)式有解，也就是(1)、(2)是有公解的.

3)如果(1)、(2)有两个解，即原来 $x$ 之外，还有 $x'$，則

$$x-x'\equiv 0(mod\ m_1), \qquad x-x'\equiv 0(mod\ m_2)$$

也就是 $x-x'$ 必須为 $m_1$、$m_2$ 的最小公倍数 $m$ 所除尽. 因而在 0 与 $m$ 之間有一个而且仅有一个 $x$ 适合于(1)、(2).

同余式有一整套的結果，和方程式一样，有"联立的"，有"高次的"等等. 当然不是这本小书所能介紹的了. 詳情將来可讀拙著"数論导引".

"3, 5, 7"算的原則可以更一般地讲成：求 $x$，使

$$x\equiv a\ (mod\ p),$$
$$x\equiv b\ (mod\ q),$$
$$x\equiv c\ (mod\ r).$$

解題法則可以讲成如果 $p, q, r$ 两两无公因子，則先求出 $A$，使

$$A\equiv 1(mod\ p),$$
$$A\equiv 0(mod\ q),$$
$$A\equiv 0(mod\ r).$$

再求出 $B$，使

$$B\equiv 0(mod\ p),$$

$$B\equiv 1(mod\ q),$$
$$B\equiv 0(mod\ r).$$

更求出 $C$, 使

$$C\equiv 0(mod\ p),$$
$$C\equiv 0(mod\ q),$$
$$C\equiv 1(mod\ r).$$

而問題的一般解是

$$x\equiv aA+bB+cC\ \ (mod\ pqr).$$

## 十一　一次不定方程

同余式

$$\left.\begin{array}{l} x\equiv 2\ \ (mod\ 3) \\ x\equiv 3\ \ (mod\ 5) \\ x\equiv 2\ \ (mod\ 7) \end{array}\right\} \qquad (1)$$

求解的問題,也可以改写成为联立方程組

$$\left.\begin{array}{l} x=2+3y \\ x=3+5z \\ x=2+7w \end{array}\right\} \qquad (2)$$

求整数解的問題. 这个方程組有三个方程,四个未知数.

一般讲来,未知数多于方程組,要求整数解的問題称为不定方程的問題. 表面上看来一次不定方程組的問題可能較同余式的問題广泛些. 但实质上他們之間是密切相关的. 其理由是: 如果要求方程組

$$ax+by+cz+dw=e,$$

$$a'x+b'y+c'z+d'w=e',$$

$$a''x+b''y+c''z+d''w=e''$$

的整数解. 用消去法, 得出

$$Ay=Bx+C,\quad A'z=B'x+C',\quad A''w=B''x+C''.$$

这便等价于同余式

$$Bx+C\equiv 0(mod\ A),\quad B'x+C'\equiv 0(mod\ A'),$$

$$B''x+C''\equiv 0(mod\ A'')$$

了.

关于不定方程, 在我国古代也有丰富的研究. 我們現在举一个例子.

"百錢买百鸡"是我国古代張丘建算經中的名題. 用現代語讲:

一百元錢买一百只鸡, 小鸡一元錢三只, 母鸡三元錢一只, 公鸡五元錢一只, 小鸡、母鸡、公鸡各几只?

这个問題的代数叙述如次:

命 $x$、$y$、$z$ 各代表小鸡、母鸡、公鸡只数, 则

$$x+y+z=100, \tag{1}$$

$$\frac{1}{3}x+3y+5z=100. \tag{2}$$

(2)×3−(1), 得出

$$8y+14z=200,$$

即

$$4y+7z=100. \tag{3}$$

用輾轉相除法, 得出

$$4\cdot 2+7(-1)=1,$$

因此 $y=200$, $z=-100$ 是方程 (3) 的一个解. 方程(3)可以改写成为

$$4y+7z=4\times 200+7\times(-100).$$

即得

$$7(z+100)=4(200-y). \tag{4}$$

由此可見 $200-y$ 是 7 的倍数, 即 $7t$, 则

$$y=200-7t, \tag{5}$$

代入(4)式

$$z=4t-100. \tag{6}$$

而

$$x=100-y-z=3t.$$

$x, y, z$ 不能是負数, 因此

$$t\geqslant 0,\ 200-7t\geqslant 0,\ 4t-100\geqslant 0,$$

即

$$\frac{200}{7}\geqslant t\geqslant 25.$$

因此, $t$ 只有 25, 26, 27, 28 四个解, 也就是

| $t$ | $x$ | $y$ | $z$ |
|---|---|---|---|
| 25 | 75 | 25 | 0 |
| 26 | 78 | 18 | 4 |
| 27 | 81 | 11 | 8 |
| 28 | 84 | 4 | 12 |

习題 1　一元錢买 15 張邮票, 其中有四分的、八分的、一

角的三种，有几种方法？

习题 2* 今有散錢不知其数，作七十七陌穿之，欠五十凑穿，若作七十八陌穿之，不多不少，問錢数若干.（严恭：通原算法(1372)）.

## 十二 原則

(3, 5, 7)算的(70, 21, 15)法提供了以下的一个原則.

要作出有性质 $A$、$B$、$C$ 的一个数学結构，而性质 $A$、$B$、$C$ 的变化又能用数据（或某种量）$\alpha$、$\beta$、$\gamma$ 来刻划，我們可用标准"单因子构件"凑成整个結构的方法：也就是先作出性质 $B$、$C$ 不发生作用而性质 $A$ 取单位量的构件，再作出性质 $C$、$A$ 不发生作用而性质 $B$ 取单位量的构件，最后作出性质 $A$、$B$ 不发生作用而性质 $C$ 取单位量的构件．所要求的結构可由这些构件凑出来.

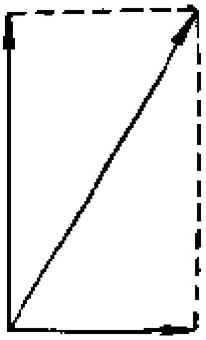
以上所用的就是这一类型的例子．我現在再举一个.

"力"可以用一个箭头来表示．箭杆的长短表示力的大小，而方向表示用力的方向.

在一点上用上两个"力"所发生的作用等于以下一个"力"的作用：以这两个"力"为边作平行四边形，这平行四边形的对角綫所表达的力.

* 这个題目的意思是：有錢一堆，每 77 个穿成一串，則少 50 个，每 78 个穿成一串，則不多不少．这堆錢有多少个？

这个力称为原来两个力的合力.



为简单計，我們只考虑同一平面上的力. 反过来，給了一个力，我們可以找出两个力，一个平行于 $x$ 軸，一个平行于 $y$ 軸，这两力的合力就等于原来所給的力.

要表出平面所有的力来，可以先作一个与 $x$ 軸平行的单位力 $f_1$，再作一个与 $y$ 軸平行的单位力 $f_2$. 任何力可以表为 $f_1$ 的 $\alpha_1$ 倍与 $f_2$ 的 $\alpha_2$ 倍所代表的力的合力.

其他的例子还很多，讀者在学习高等数学的时候会不断发現的.

# 附記　孙子算經

孙子算經是我国古代的优秀著作，但是作者和出版年代都无法考证了.

有人說：这是孙武的作品(也就是写兵法书孙子十三篇的作者). 但也有人反对. 有人根据其中的内容論断，认为是汉魏时人. 例如，清代戴震就根据书中涉及到"长安洛阳的距离"和"佛书二十九章"等語，断定为汉明帝以后的人. 又如，清代阮元根据其中有棊局十九道，而断定为汉以后的人. 但也有人反对这些意見，因为古代常有在一本名著重新刊印的时候摻杂了若干后人的补充材料. 因此，作者和年代(实质上，不止年代，应当說那个世紀)都还是不能确定的問題(从战国到三国).

纵然如此，它仍然是我国最古老的数学三名著之一：即周髀算經，九章算术与孙子算經，特别是"物不知其数"一题是世界上公认的古老的重要的工作.